EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1139	380/277.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 11:27
L2	453	380/278.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 11:27
L3	277	380/282.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:07
L4	607	713/150.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:07
L5	687	713/153.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:07
L6	747	713/155.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08
L7	752	705/64.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08
L8	493	705/75.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08
L9	295	705/76.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08

EAST Search History

L10	0	705/777.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08
L11	170	705/77.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:08
L12	187	705/78.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:53
L13	441	(identi$4 adj5 based) with (encrypt$3 or encipher$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:57
L14	124	l13 same ((public adj3 key) or asymmetric)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 12:58
L15	41	(l1 or l2 or l4 or l5 or l6 or l7 or l8) and l13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 13:22
L16	61	l14 and (Weil or tate or (quadratic adj3 residu$5) or (bilinear adj5 (map$5 or pair$4)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/12/26 13:24

Results for "**(identity based encryption<in>metadata)**":

e-mail

Your search matched **16** of **1450046** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(identity based encryption<in>metadata) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Securing e-mail with identity-based encryption**
McCullagh, N.;
IT Professional
Volume 7, Issue 3, May-June 2005 Page(s):64, 61 - 63
Digital Object Identifier 10.1109/MITP.2005.70
AbstractPlus | Full Text: PDF(704 KB) IEEE JNL
Rights and Permissions

2. **Faster identity based encryption**
Scott, M.;
Electronics Letters
Volume 40, Issue 14, 8 July 2004 Page(s):861 - 862
Digital Object Identifier 10.1049/el:20045081
AbstractPlus | Full Text: PDF(192 KB) IEE JNL

3. **Exploiting Hierarchical Identity-Based Encryption for Access Control to F Computing Information**
Hengartner, U.; Steenkiste, P.;
Security and Privacy for Emerging Areas in Communications Networks, 2005. 2005. First International Conference on
05-09 Sept. 2005 Page(s):384 - 396
Digital Object Identifier 10.1109/SECURECOMM.2005.18
AbstractPlus | Full Text: PDF(376 KB) IEEE CNF
Rights and Permissions

4. **A new scheme for securing mobile agents**
Malek, B.; Miri, A.;
Electrical and Computer Engineering, 2004. Canadian Conference on
Volume 3, 2-5 May 2004 Page(s):1699 - 1702 Vol.3
AbstractPlus | Full Text: PDF(488 KB) IEEE CNF
Rights and Permissions

5. **Secure communication in a distributed system using identity based encr**
Stading, T.;
Cluster Computing and the Grid, 2003. Proceedings. CCGrid 2003. 3rd IEEE/A Symposium on
12-15 May 2003 Page(s):414 - 420
Digital Object Identifier 10.1109/CCGRID.2003.1199395
AbstractPlus | Full Text: PDF(263 KB) IEEE CNF
Rights and Permissions

6. **Fitting Square Pegs into Round Holes**
Martin, L.;
Security & Privacy Magazine, IEEE
Volume 4, Issue 5, Sept.-Oct. 2006 Page(s):64 - 66
Digital Object Identifier 10.1109/MSP.2006.120
AbstractPlus | Full Text: PDF(403 KB) IEEE JNL
Rights and Permissions

7. **Achieving energy efficient and secure communication in wireless sensor**
Praveena, A.; Devasena, S.; Chelvan, K.M.A.;
Wireless and Optical Communications Networks, 2006 IFIP International Confe
11-13 April 2006 Page(s):5 pp.
Digital Object Identifier 10.1109/WOCN.2006.1666571
AbstractPlus | Full Text: PDF(4056 KB) IEEE CNF
Rights and Permissions

8. **The advantages of elliptic curve cryptography for wireless security**
Lauter, K.;
Wireless Communications, IEEE [see also IEEE Personal Communications]
Volume 11, Issue 1, Feb 2004 Page(s):62 - 67
Digital Object Identifier 10.1109/MWC.2004.1269719
AbstractPlus | Full Text: PDF(247 KB) IEEE JNL
Rights and Permissions

9. **Personalized service mobility and security in SIP-based communications**
Dafu Lou; Dongmei Jiang; Tet Yeap; O'Brian, W.;
Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Co
Communication., 2005 13th IEEE International Conference on
Volume 1, 16-18 Nov. 2005 Page(s):5 pp.
Digital Object Identifier 10.1109/ICON.2005.1635450
AbstractPlus | Full Text: PDF(3728 KB) IEEE CNF
Rights and Permissions

10. **Towards accountable management of identity and privacy: sticky policie enforceable tracing services**
Mont, M.C.; Pearson, S.; Bramhall, P.;
Database and Expert Systems Applications, 2003. Proceedings. 14th Internati
1-5 Sept. 2003 Page(s):377 - 382
Digital Object Identifier 10.1109/DEXA.2003.1232051
AbstractPlus | Full Text: PDF(232 KB) IEEE CNF
Rights and Permissions

11. **Exposure-resilience for free: the hierarchical ID-based encryption case**
Dodis, Y.; Yung, M.;
Security in Storage Workshop, 2002. Proceedings. First International IEEE
11 Dec. 2002 Page(s):45 - 52
AbstractPlus | Full Text: PDF(379 KB) IEEE CNF
Rights and Permissions

12. **A Fault Attack on Pairing-Based Cryptography**
Page, D.; Vercauteren, F.;
Computers, IEEE Transactions on
Volume 55, Issue 9, Sept. 2006 Page(s):1075 - 1080
Digital Object Identifier 10.1109/TC.2006.134
AbstractPlus | Full Text: PDF(152 KB) IEEE JNL
Rights and Permissions

13. **An ID-based broadcast encryption scheme for key distribution**
Xinjun Du; Ying Wang; Jianhua Ge; Yumin Wang;
Broadcasting, IEEE Transactions on
Volume 51, Issue 2, June 2005 Page(s):264 - 266
Digital Object Identifier 10.1109/TBC.2005.847600
AbstractPlus | References | Full Text: PDF(120 KB) IEEE JNL

Rights and Permissions

14. **AMPol: Adaptive Messaging Policy**
Raja Afandi; Jianqing Zhang; Munawar Hafiz; Gunter;
Web Services, 2006. ECOWS '06. 4th European Conference on
Dec. 2006 Page(s):53 - 64
Digital Object Identifier 10.1109/ECOWS.2006.9
AbstractPlus | Full Text: PDF(1003 KB) IEEE CNF
Rights and Permissions

15. **Secure Web Service Discovery: Overcoming Challenges of Ubiquitous C**
Trabelsi, S.; Pazzaglia, J.-C.; Roudier, Y.;
Web Services, 2006. ECOWS '06. 4th European Conference on
Dec. 2006 Page(s):35 - 43
Digital Object Identifier 10.1109/ECOWS.2006.33
AbstractPlus | Full Text: PDF(272 KB) IEEE CNF
Rights and Permissions

16. **A Promenade through the New Cryptography of Bilinear Pairings**
Boyen, X.;
Information Theory Workshop, 2006 IEEE
2006 Page(s):19 - 23
Digital Object Identifier 10.1109/ITW.2006.1633773
AbstractPlus | Full Text: PDF(1656 KB) IEEE CNF
Rights and Permissions

Terms used **identity based encryption** Found **57** of **193,448**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 57 Result page: 1 2 3 next

Relevance scale

1 Applications II: An Identity Based Encryption system

Louise Owens, Adam Duffy, Tom Dowling

June 2004 **Proceedings of the 3rd international symposium on Principles and practice of programming in Java PPPJ '04**

Publisher: Trinity College Dublin

Full text available: pdf(380.76 KB) Additional Information: full citation, abstract, references

We describe an Identity Based Encryption (IBE) cryptosystem based on a scheme presented by Boneh and Franklin [3]. We implement the abstract mathematical concepts underlying this system. We reuse an existing Elliptic curve arithmetic API, [4] to reduce the development time of the IBE system. We present a Java Cryptographic Architecture (JCA) integrated implementation of IBE that will allow Java developers to easily take advantage of this new encryption system and thus eliminate some of the most ...

2 Cryptography: Direct chosen ciphertext security from identity-based techniques

Xavier Boyen, Qixiang Mei, Brent Waters

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

Publisher: ACM Press

Full text available: pdf(305.35 KB) Additional Information: full citation, abstract, references, index terms

We describe a new encryption technique that is secure in the standard model against chosen ciphertext attacks. We base our method on two very efficient Identity-Based Encryption (IBE) schemes without random oracles due to Boneh and Boyen, and Waters.Unlike previous CCA2-secure cryptosystems that use IBE as a black box, our approach is very simple and compact. It makes direct use of the underlying IBE structure, and requires no cryptographic primitive other than the IBE scheme itself. This convey ...

Keywords: chosen ciphertext security, identity-based encryption

3 Data protection: Attribute-based encryption for fine-grained access control of encrypted data

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

Publisher: ACM Press

Full text available: pdf(277.46 KB) Additional Information: full citation, abstract, references, index terms

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data

that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and pri ...

Keywords: access control, attribute-based encryption, audit logs, broadcast encryption, delegation, hierarchical identity-based encryption

4 Industry track invited talks: Identity-based encryption from algorithm to enterprise deployment

Guido Appenzeller

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

Publisher: ACM Press

Full text available: pdf(107.96 KB) Additional Information: full citation, abstract, index terms

Identity-Based encryption is an asymmetric encryption system where identifiers such as email addresses, server names or phone numbers, can be used as public keys. Originally proposed by Adi Shamir in 1984, the first practical algorithm became available in 2001. Since then IBE has not only generated huge interest in academia, it has seen wide-scale adoption in industry, is used by hundreds of thousands of users and is in the process of being standardized by the IEEE.In this talk we will give an o ...

5 New basic technologies for DIM: Pseudonym management using mediated identity-based cryptography

Thibault Candebat, Cameron Ross Dunne, David T. Gray

November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM '05**

Publisher: ACM Press

Full text available: pdf(293.16 KB) Additional Information: full citation, abstract, references, index terms

Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone users who may need to supply their identity and location information to untrustworthy third parties in order to access these applications. Widespread acceptance of such services may therefore depend on how privacy sensitive information will be handled in order to restore users' confidence in what could become the "killer app" of 3G networks. In this paper, we present a proxy-based public key infrastructure tha ...

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymity

6 Efficient revocation and threshold pairing based cryptosystems

Benoît Libert, Jean-Jacques Quisquater

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**

Publisher: ACM Press

Full text available: pdf(1.02 MB) Additional Information: full citation, abstract, references, index terms

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRS ...

Keywords: Public key cryptosystems, bilinear maps, revocation

7 Cryptographic tools: ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption

Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(220.00 KB) Additional Information: full citation, abstract, references, index terms

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys with time. Forward security has several unique requirements in hierarchical identity-based encryption (HIBE) scheme: (1) users join dynamically; (2) encryption is joining-time-oblivious; (3) users evolve secret keys autonomously.

We present a scalable forward-secure HIBE (fs-HIBE) scheme satisfying the above properties. We also show how our fs-HIBE scheme can be used to construct a forward-secure ...

Keywords: ID-Based encryption, broadcast encryption, forward security

8 Applied cryptography I: Forward-secure signatures with untrusted update
Xavier Boyen, Hovav Shacham, Emily Shen, Brent Waters
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(261.19 KB) Additional Information: full citation, abstract, references, index terms

In most forward-secure signature constructions, a program that updates a user's private signing key must have full access to the private key. Unfortunately, these schemes are incompatible with several security architectures including Gnu Privacy Guard (GPG) and S/MIME, where the private key is encrypted under a user password as a "second factor" of security, in case the private key storage is corrupted, but the password is not.We introduce the concept of forward-secure signatures with untrusted ...

Keywords: digital signatures, forward security, two-factor authentication, untrusted storage

9 Oblivious signature-based envelope
Ninghui Li, Wenliang Du, Dan Boneh
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**
Publisher: ACM Press
Full text available: pdf(874.99 KB) Additional Information: full citation, abstract, references, citings, index terms

Exchange of digitally signed certificates is often used to establish mutual trust between strangers that wish to share resources or to conduct business transactions. Automated Trust Negotiation (ATN) is an approach to regulate the flow of sensitive information during such an exchange. Previous work on ATN are based on access control techniques, and cannot handle cyclic policy interdependency satisfactorily. We show that the problem can be modelled as a 2-party secure function evaluation (SFE) pr ...

10 Securing IPv6 neighbor and router discovery
Jari Arkko, Tuomas Aura, James Kempf, Vesa-Matti Mäntylä, Pekka Nikander, Michael Roe
September 2002 **Proceedings of the 3rd ACM workshop on Wireless security WiSE '02**
Publisher: ACM Press
Full text available: pdf(113.58 KB) Additional Information: full citation, abstract, references, citings, index terms

When IPv6 Neighbor and Router Discovery functions were defined, it was assumed that the local link would consist of mutually trusting nodes. However, the recent developments in public wireless networks, such as WLANs, have radically changed the situation. The

nodes on a local link cannot necessarily trust each other any more, but they must become mutually suspicious even when the nodes have completed an authentication exchange with the network. This creates a number of operational difficulties a ...

Keywords: autoconfiguration, detection, duplicate address, identity-based cryptosystems, neighbor discovery, router discovery

11 Credentials: Concealing complex policies with hidden credentials

Robert W. Bradshaw, Jason E. Holt, Kent E. Seamons
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(219.13 KB) Additional Information: full citation, abstract, references, index terms

Hidden credentials are useful in protecting sensitive resource requests, resources, policies, and credentials. We propose a significant performance improvement when implementing hidden credentials using Boneh/Franklin Identity Based Encryption. We also propose a substantially improved secret splitting scheme for enforcing complex policies, and show how it improves concealment of policies from nonsatisfying recipients.

Keywords: authentication, credentials, identity based encryption, privacy, secret sharing, trust negotiation

12 Data protection: Secure attribute-based systems

Matthew Pirretti, Patrick Traynor, Patrick McDaniel, Brent Waters
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(1.13 MB) Additional Information: full citation, abstract, references, index terms

Attributes define, classify, or annotate the datum to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In this paper, we introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those polic ...

Keywords: applied cryptography, attribute-based encryption, secure systems

13 Fine-grained control of security capabilities

Dan Boneh, Xuhua Ding, Gene Tsudik
February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1
Publisher: ACM Press
Full text available: pdf(128.09 KB) Additional Information: full citation, abstract, references, index terms

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure

14 Usability: Moving from the design of usable security technologies to the design of useful secure applications

D. K. Smetters, R. E. Grinter
September 2002 **Proceedings of the 2002 workshop on New security paradigms**
Publisher: ACM Press

Full text available: pdf(795.12 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent results from usability studies of security systems have shown that end-users find them difficult to adopt and use. In this paper we argue that improving the usability of security technology is only one part of the problem, and that what is missed is the need to design usable and useful systems that provide security to end-users in terms of the applications that they use and the tasks they want to achieve. We propose alternate ways of building and integrating security technologies into app ...

Keywords: usable security

15 An efficient identity-based signature scheme with batch verifications

Shi Cui, Pu Duan, Choong Wah Chan
May 2006 **Proceedings of the 1st international conference on Scalable information systems InfoScale '06**
Publisher: ACM Press
Full text available: pdf(134.08 KB) Additional Information: full citation, abstract, references

Mapping messages or a user's identity into a point on elliptic curves is required by many pairing-based cryptographic schemes. In most of pairing-based schemes, this requirement is realized by a special hash function, *MapToPoint* function. However, the efficiency of the *MapToPoint* function is much lower than the general hash functions. In this paper, we propose a new identity-based signature (IBS) scheme without *MapToPoint* function which speeds up extracting secret key and ve ...

16 Dynamic Access Control: An access control model for dynamic client-side content

Adam Hess, Kent E. Seamons
June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies**
Publisher: ACM Press
Full text available: pdf(608.50 KB) Additional Information: full citation, abstract, references, index terms

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources are usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this paper, we turn the traditional client/server access control model on its head, and address how to protect the sensitive content that clients disclose to serve ...

Keywords: access control, authentication, credentials, trust negotiation

17 Data integrity: The HP time vault service: exploiting IBE for timed release of confidential information

Marco Casassa Mont, Keith Harrison, Martin Sadler
May 2003 **Proceedings of the 12th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(860.87 KB) Additional Information: full citation, abstract, references, index terms

Digital information is increasingly more and more important to enable interactions and transactions on the Internet. On the other hand, leakages of sensitive information can have harmful effects for people, enterprises and governments.This paper focuses on the problems of dealing with timed release of confidential information and simplifying its access once public: it is a common issue in the industry, government and day-to-day

life.We introduce the "HP Time Vault Service", based on the emerging ...

Keywords: disclosure policies, identifier-based encryption, privacy, security, timed-release, web service

18 Credential-based access control and data privacy: Hidden Credentials

Jason E. Holt, Robert W. Bradshaw, Kent E. Seamons, Hilarie Orman
October 2003 **Proceedings of the 2003 ACM workshop on Privacy in the electronic society**
Publisher: ACM Press

Full text available: pdf(139.28 KB) Additional Information: full citation, abstract, references, citings, index terms

Hidden Credentials are useful in situations where requests for service, credentials, access policies and resources are extremely sensitive. We show how transactions which depend on fulfillment of policies described by monotonic boolean formulae can take place in a single round of messages. We further show how credentials that are never revealed can be used to retrieve sensitive resources.

Keywords: authentication, credentials, identity based encryption, privacy, trust negotiation

19 Secure routing and firewall: Identity-based registry for secure interdomain routing

E-yong Kim, Klara Nahrstedt, Li Xiao, Kunsoo Park
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(320.80 KB) Additional Information: full citation, abstract, references, index terms

The current Internet has no secure way to validate the correctness of the routing information. We suggest a mechanism that supports secure validation of routing information in the interdomain routing protocol of the Internet. Our mechanism focuses on alleviating obstacles which previously prevent the complete and correct construction of the Internet routing information. In particular, we propose an *identity-based Registry with Authorized and Verifiable Search* (RAVS) so that routing inform ...

Keywords: authorized search, identity-based registry, verifiable search

20 Supporting cryptographic technology: New traitor tracing schemes using bilinear map

V. D. Tô, R. Safavi-Naini, F. Zhang
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(226.82 KB) Additional Information: full citation, abstract, references, index terms

Mitsunari et al [15] presented a new traitor tracing scheme which uses Weil pairing in elliptic curves. To the best of our knowledge this is the first scheme that uses bilinear map. The claimed advantage of the scheme is that the ciphertext size is independent of the number of traitors. It is shown that the problem of constructing a pirate key by k colluders is as hard as the so-called "k-weak Diffie-Hellman problem".In this paper, we show an attack on this scheme in which traitors ...

Keywords: bilinear map, elliptic curve, revocation, traitor tracing

Terms used **identity based encryption** Found **57** of **193,448**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 21 - 40 of 57 Result page: previous 1 2 3 next

Relevance scale

21 Cryptology II: ID-based threshold decryption without random oracles and its application in key escrow

Zhenchuan Chai, Zhenfu Cao, Rongxing Lu
November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**
Publisher: ACM Press
Full text available: pdf(514.58 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we first present an ID-based threshold decryption scheme *ThD* based on bilinear Diffie-Hellman inversion assumption, and prove that it is selective chosen plaintext secure without random oracles. Then, we enhance *ThD* to a more secure level with ciphertext validation test before decryption. At last, we apply *ThD* to key escrow, resulting in a robust threshold key escrow system.

Keywords: ID-based cryptography, key escrow, threshold decryption

22 Cryptology I: Robust ID-based threshold signcryption scheme from pairings

Shanshan Duan, Zhenfu Cao, Rongxing Lu
November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**
Publisher: ACM Press
Full text available: pdf(379.31 KB) Additional Information: full citation, abstract, references, index terms

Recently bilinear pairings on elliptic curves have raised great interest in cryptographic community. Based on their good properties, many excellent ID-based cryptographic schemes have been proposed. However, in these proposed schemes, the private key generator should be assumed trusted, while in real environment, this assumption does not always hold. To overcome this weakness, in this paper, we will use the threshold technology to devise a secure ID-based signcryption scheme. Since the threshold ...

Keywords: bilinear pairings, identity-based cryptography, signcryption, threshold scheme

23 Content-triggered trust negotiation

Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons
August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3
Publisher: ACM Press
Full text available: pdf(815.36 KB) Additional Information: full citation, abstract, references, index terms

The focus of access control in client/server environments is on protecting sensitive server

resources by determining whether or not a client is authorized to access those resources. The set of resources is usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this article, we turn the traditional client/server access control model on its head and address how to protect the sensitive content that clients disclose to and r ...

Keywords: Trust negotiation, access control, authentication, credentials

24 Puzzles and users: New client puzzle outsourcing techniques for DoS resistance

Brent Waters, Ari Juels, J. Alex Halderman, Edward W. Felten
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(382.11 KB) Additional Information: full citation, abstract, references, index terms

We explore new techniques for the use of cryptographic puzzles as a countermeasure to Denial-of-Service (DoS) attacks. We propose simple new techniques that permit the outsourcing of puzzles; their distribution via a robust external service that we call a bastion. Many servers can rely on puzzles distributed by a single bastion. We show how a bastion, somewhat surprisingly, need not know which servers rely on its services. Indeed, in one of our constructions, a bastion may consist merely of ...

Keywords: DoS, client puzzles, denial-of-service

25 Short papers: Hidden access control policies with hidden credentials

Keith Frikken, Mikhail Atallah, Jiangtao Li
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**
Publisher: ACM Press
Full text available: pdf(49.57 KB) Additional Information: full citation, abstract, references, index terms

In an open environment such as the Internet, the decision to collaborate with a stranger (e.g., by granting access to a resource) is often based on the characteristics (rather than the identity) of the requester, via digital credentials: Access is granted if Alice's credentials satisfy Bob's access policy. The literature contains many scenarios in which it is desirable to carry out such trust negotiations in a privacy-preserving manner, i.e., so as minimize the disclosure of credentials and/o ...

Keywords: access control, hidden credentials, privacy, secure multi-party computation, trust negotiation

26 Sensors and networking: Provably-secure time-bound hierarchical key assignment schemes

Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(311.76 KB) Additional Information: full citation, abstract, references, index terms

A *time-bound hierarchical key assignment scheme* is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that the key of a higher class can be used to derive the keys of all classes lower down in the hierarchy, according to temporal constraints.In this paper we design and analyze time-bound hierarchical key assignment schemes which are provably-secure and efficient. We first consider the *unconditionally secure setting* ...

Keywords: access control, key assignment, provable security

27 New topics: Low-cost communication for rural internet kiosks using mechanical backhaul

A. Seth, D. Kroeker, M. Zaharia, S. Guo, S. Keshav
September 2006 **Proceedings of the 12th annual international conference on Mobile computing and networking MobiCom '06**
Publisher: ACM Press
Full text available: pdf(733.95 KB) Additional Information: full citation, abstract, references, index terms

Rural kiosks in developing countries provide a variety of services such as birth, marriage, and death certificates, electricity bill collection, land records, email services, and consulting on medical and agricultural problems. Fundamental to a kiosk's operation is its connection to the Internet. Network connectivity today is primarily provided by dialup telephone, although Very Small Aperture Terminals (VSAT) or long-distance wireless links are also being deployed. These solutions tend to be bo ...

Keywords: delay tolerant networks, low cost, mechanical back-haul, rural communication, system design

28 Broadcast: Reliable broadcast in unknown fixed-identity networks

Lakshminarayanan Subramanian, Randy H. Katz, Volker Roth, Scott Shenker, Ion Stoica
July 2005 **Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing PODC '05**
Publisher: ACM Press
Full text available: pdf(308.90 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we formulate a new theoretical problem, namely the *reliable broadcast problem in unknown fixed-identity networks*. This problem arises in the context of developing decentralized security mechanisms in a specific-class of distributed systems: Consider an undirected graph *G* connecting *n* nodes where each node is *aware of only its neighbors* but not of the entire graph. Additionally, each node has a *unique identity* and cannot fake its identity to its n ...

Keywords: byzantine agreement, reliable broadcast, unknown network

29 Database security: Publicly verifiable ownership protection for relational databases

Yingjiu Li, Robert Huijie Deng
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(332.50 KB) Additional Information: full citation, abstract, references, index terms

Today, watermarking techniques have been extended from the multimedia context to relational databases so as to protect the ownership of data even after the data are published or distributed. However, all existing watermarking schemes for relational databases are *secret key based,* thus require a secret key to be presented in proof of ownership. This means that the ownership can only be proven once to the public (e.g., to the court). After that, the secret key is known to the public and the ...

Keywords: certificate, ownership protection, public verifiability, relational database, watermark

30 Computer security (SEC): SELS: a secure e-mail list service

Himanshu Khurana, Adam Slagell, Rafael Bonilla
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**
Publisher: ACM Press
Full text available: pdf(218.91 KB) Additional Information: full citation, abstract, references, index terms

Exchange of private information content among a large number of users via *E-mail List Services* is becoming increasingly common. In this paper we address security requirements in that setting and develop a new protocol, SELS (a Secure E-mail List Service) that provides confidentiality, integrity, and authentication for e-mails exchanged via lists. In addition, SELS also protects against the use of lists for e-mail spamming. We have developed a prototype of SELS in Java, and integrated it w ...

Keywords: electronic mail, mailing list, security

31 Supporting cryptographic technology: Broadcast encryption with short keys and transmissions

Nuttapong Attrapadung, Kazukuni Kobara

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(269.23 KB) Additional Information: full citation, abstract, references, citings, index terms

Broadcast Encryption allows a broadcaster to broadcast an encrypted message so that only a dynamically changing designated group of users can decrypt it. The stateless setting considers the case where the private key at each user is never updated. A central open problem in this area is to design a stateless scheme where both the size of transmission header which encapsulates the session key and the size of private key at each user are small and *independent* of the number of users (all/priv ...

Keywords: broadcast encryption, constant transmission rate, copyright protection, one-way accumulators, revocation scheme

32 Supporting cryptographic technology: Breaking and repairing optimistic fair exchange from PODC 2003

Yevgeniy Dodis, Leonid Reyzin

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(150.75 KB) Additional Information: full citation, abstract, references, citings, index terms

In PODC 2003, Park, Chong, Siegel and Ray [22] proposed an optimistic protocol for fair exchange, based on RSA signatures. We show that their protocol is *totally breakable* already in the registration phase: the honest-but-curious arbitrator can easily determine the signer's secret key.On a positive note, the authors of [22] informally introduced a connection between fair exchange and "sequential two-party multisignature schemes" (which we call *two-signatures*), but used an insecure ...

Keywords: digital signatures, fair exchange, multisignatures, verifiably committed signatures, verifiably encrypted signatures

33 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of

BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

34 Access management for distributed systems: Role-based cascaded delegation

Roberto Tamassia, Danfeng Yao, William H. Winsborough
June 2004 **Proceedings of the ninth ACM symposium on Access control models and technologies**
Publisher: ACM Press

Full text available: pdf(218.61 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose *role-based cascaded delegation*, a model for delegation of authority in decentralized trust management systems. We show that role-based cascaded delegation combines the advantages ofrole-based trust management with those of cascaded delegation. We also present an efficient and scalable implementation of role-based cascaded delegation using Hierarchical Certificate-Based Encryption, where the authentication information for an arbitrarily long role-based delegation chain is captur ...

Keywords: RBAC, access control, delegation, trust management

35 Poster paper sessions: Identity-based confirmer signatures from pairings over elliptic curves

Song Han, Winson K.Y. Yeung, Jie Wang
June 2003 **Proceedings of the 4th ACM conference on Electronic commerce**
Publisher: ACM Press
Full text available: pdf(127.14 KB) Additional Information: full citation, abstract, references, index terms

We propose a new identity-based signature scheme from Weil pairing or Tate pairing. We prove that the confirmation and denial protocols of our scheme have the completeness and soundness properties. Our scheme is efficient in computation.

Keywords: Weil pairing, computational Diffie-Hellman problem, elliptic curve discrete logarithms, identity-based signatures

36 Cryptographic tools: The dual receiver cryptosystem and its applications

Theodore Diament, Homin K. Lee, Angelos D. Keromytis, Moti Yung
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(329.14 KB) Additional Information: full citation, abstract, references, index terms

We put forth the notion of a dual receiver cryptosystem and implement it based on bilinear pairings over certain elliptic curve groups. The cryptosystem is simple and efficient yet powerful, as it solves two problems of practical importance whose solutions have proven to be elusive before:(1) A provably secure "combined" public-key cryptosystem (with a single secret key per user in space-limited environment) where the key is used for both decryption and signing and where encryption can be esc ...

Keywords: digital signature, elliptic curves, key escrow, pairing-based cryptography, public key, puzzles, useful secure computation

37 SecCMP: a secure chip-multiprocessor architecture

Li Yang, Lu Peng

October 2006 **Proceedings of the 1st workshop on Architectural and system support for improving software dependability ASID '06**
Publisher: ACM Press
Full text available: pdf(419.78 KB) Additional Information: full citation, abstract, references, index terms

Security has been considered as an important issue in processor design. Most of the existing mechanisms address security and integrity issues caused by untrusted main memory in single-core systems. In this paper, we propose a secure Chip-Multiprocessor architecture (*SecCMP*) to handle security related problems such as key protection and core authentication in multi-core systems. Threshold secret sharing scheme is employed to protect critical keys because secret sharing is a distributed sec ...

Keywords: chip-multiprocessor, encryption, fault-tolerance, security

38 Applied cryptography II: Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation
Mihir Bellare, Tadayoshi Kohno, Victor Shoup
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(235.26 KB) Additional Information: full citation, abstract, references, index terms

We show how to significantly speed-up the encryption portion of some public-key cryptosystems by the simple expedient of allowing a sender to maintain state that is re-used across different encryptions.In particular we present stateful versions of the DHIES and Kurosawa-Desmedt schemes that each use only 1 exponentiation to encrypt, as opposed to 2 and 3 respectively in the original schemes, yielding the fastest discrete-log based public-key encryption schemes known in the random-oracle and stan ...

Keywords: cryptography, public-key encryption

39 Applied cryptography I: A fully collusion resistant broadcast, trace, and revoke system
Dan Boneh, Brent Waters
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(256.37 KB) Additional Information: full citation, abstract, references, index terms

We introduce a simple primitive called *Augmented Broadcast Encryption* (ABE) that is sufficient for constructing broadcast encryption, traitor-tracing, and trace-and-revoke systems. These ABE-based constructions are resistant to an arbitrary number of colluders and are secure against *adaptive adversaries*. Furthermore, traitor tracing requires no secrets and can be done by anyone. These broadcast systems are designed for broadcasting to arbitrary sets of users. We then construct a se ...

40 Applied cryptography I: How to win the clonewars: efficient periodic n-times anonymous authentication
Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, Mira Meyerovich
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(313.55 KB) Additional Information: full citation, abstract, references, index terms

We create a credential system that lets a user anonymously authenticate at most n times in a single time period. A user withdraws a dispenser of *n* e-tokens. She shows an e-token to a verifier to authenticate herself; each e-token can be used only once, however, the dispenser automatically refreshes every time period. The only prior solution to this problem, due to Damgård et al. [29], uses protocols that are a factor of *k* slower

for the user and verifier, where *k* is t ...

Keywords: *n*-anonymous authentication, clone detection, credentials

Results 21 - 40 of 57 Result page: previous 1 **2** 3 next

Terms used **identity based encryption** Found **57** of **193,448**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 41 - 57 of 57 Result page: previous 1 2 3

Relevance scale

41 Authentication: Message authentication by integrity with public corroboration

P. C. van Oorschot
September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**
Publisher: ACM Press
Full text available: pdf(2.31 MB) Additional Information: full citation, abstract, references, index terms

One of the best-known security paradigms is to use authentication as the basis for access control decisions. We turn this around, and instead rely on access control (or more precisely, integrity) as the basis for authentication. We propose a simple, practical means by which data origin assurances for message authentication are based on corroboration, for example by cross-checking with information made available by a known source or at a specified location (e.g., web page). The security re ...

Keywords: data origin authentication, digital signatures, email source authentication, message authentication, phishing, security by integrity, spam, undetected key compromise

42 Secure and security systems: Software implementation of Tate pairing over GF(2^m)

G. Bertoni, L. Breveglieri, P. Fragneto, G. Pelosi, L. Sportiello
March 2006 **Proceedings of the conference on Design, automation and test in Europe: Designers' forum DATE '06**
Publisher: European Design and Automation Association
Full text available: pdf(170.58 KB) Additional Information: full citation, abstract, references

Recently, the interest about the Tate pairing over binary fields has decreased due to the existence of efficient attacks to the discrete logarithm problem in the subgroups of such fields. We show that the choice of fields of large size to make these attacks infeasible does not lead to a degradation of the computation performance of the pairing. We describe and evaluate by simulation an implementation of the Tate pairing that allows to achieve good timing results, comparable with those reported i ...

43 Secure routing and firewall: Digitally signed document sanitizing scheme based on bilinear maps

Kunihiko Miyazaki, Goichiro Hanaoka, Hideki Imai
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(565.33 KB) Additional Information: full citation, abstract, references, index terms

A digital signature does not allow any alteration of the document to which it is attached. Appropriate alteration of some signed documents, however, should be allowed because

there are security requirements other than the integrity of the document. In the disclosure of official information, for example, sensitive information such as personal information or national secrets is masked when an official document is sanitized so that its nonsensitive information can be disclosed when it is requested ...

Keywords: digital signature, information disclosure, privacy issue

44 Security protocols: Designated group credentials

Ching Yu Ng, Willy Susilo, Yi Mu

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(295.78 KB) Additional Information: full citation, abstract, references, index terms

Consider a situation where a secret agent wants to authenticate herself to the other secret agents. This secret agent must be able to convince the others of her identity. She cannot convince any other people other than those predetermined secret agents. This is to avoid problems that might occur if this secret agent would like to 'betray' her group. On the whole we would like to allow the agent to convince a predetermined group of people by showing that she holds a credential and so she is a mem ...

Keywords: bilinear pairings, credential, designated, signature

45 Improved proxy re-encryption schemes with applications to secure distributed storage

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger

February 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM Press

Full text available: pdf(331.59 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

46 Access control to people location information

Urs Hengartner, Peter Steenkiste

November 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 4

Publisher: ACM Press

Full text available: pdf(356.85 KB) Additional Information: full citation, abstract, references, index terms

Ubiquitous computing uses a variety of information for which access needs to be controlled. For instance, a person's current location is a sensitive piece of information that only authorized entities should be able to learn. Several challenges arise in the specification and implementation of policies controlling access to location information. For example, there can be multiple sources of location information. The sources can be within different administrative domains, which might allow differen ...

Keywords: Certificates, DSA, RSA, SPKI/SDSI, credential discovery, delegation, location, privacy, trust

47 Cryptographic storage security: Key management for multi-user encrypted databases

Ernesto Damiani, S. De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(408.91 KB) Additional Information: full citation, abstract, references, index terms

Database outsourcing is becoming increasingly popular introducing a new paradigm, called *database-as-a-service* (DAS), where an organization's database is stored at an external service provider. In such a scenario, access control is a very important issue, especially if the data owner wishes to publish her data for external use.In this paper, we first present our approach for the implementation of access control through selective encryption. The focus of the paper is then the presentation ...

Keywords: encrypted/indexing databases, hierarchical key derivation schema, selective access

48 Short papers -- storage survivability: Toward securing untrusted storage without public-key operations
Dalit Naor, Amir Shenhav, Avishai Wool
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(344.77 KB) Additional Information: full citation, abstract, references, index terms

Adding security capabilities to shared, remote and untrusted storage file systems leads to performance degradation that limits their use. Public-key cryptographic primitives, widely used in such file systems, are known to have worse performance than their symmetric key counterparts. In this paper we examine design alternatives that avoid public-key cryptography operations to achieve better performance. We present the trade-offs and limitations that are introduced by these substitutions.

Keywords: network attached storage, secure file systems

49 Cryptography: Proxy re-signatures: new definitions, algorithms, and applications
Giuseppe Ateniese, Susan Hohenberger
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(225.25 KB) Additional Information: full citation, abstract, references, index terms

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed *proxy re-signatures*, in which a semi-trusted proxy acts as a *translator* between Alice and Bob. To translate, the proxy converts a signature from Alice into a signature from Bob on the same message. The proxy, however, does not learn any signing key and cannot sign arbitrary messages on behalf of either Alice or Bob. Since the BBS proposal, the proxy re-signature primitive has been largely ignored, but we show that it is a very use ...

Keywords: authenticating path in network, bilinear maps, proxy re-signature

50 Authentication: Aggregated path authentication for efficient BGP security
Meiyuan Zhao, Sean W. Smith, David M. Nicol
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(136.63 KB) Additional Information: full citation, abstract, references, index terms

The *Border Gateway Protocol (BGP)* controls inter-domain routing in the Internet. BGP is

vulnerable to many attacks, since routers rely on hearsay information from neighbors. *Secure BGP (S-BGP)* uses DSA to provide route authentication and mitigate many of these risks. However, many performance and deployment issues prevent S-BGP's real-world deployment. Previous work has explored improving S-BGP processing latencies, but space problems, such as increased message size and memory cost ...

Keywords: BGP, authentication, performance, routing, security

51 Privacy and anonymity: Untraceable RFID tags via insubvertible encryption

Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(238.38 KB) Additional Information: full citation, abstract, references, index terms

We introduce a new cryptographic primitive, called *insubvertible encryption*, that produces ciphertexts which can be randomized without the need of any key material. Unlike plain universal re-encryption schemes, insubvertible encryption prevents against adversarial exploitation of hidden channels, by including certificates proving that the ciphertext can only be decrypted by authorized parties.The scheme can be applied to RFID tags, providing strong protection against tracing. This enables ...

Keywords: RFID privacy, bilinear maps, universal re-encryption

52 Technical papers: An efficient group key establishment in location-aided mobile ad hoc networks

Depeng Li, Srinivas Sampalli
October 2005 **Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks PE-WASUN '05**
Publisher: ACM Press
Full text available: pdf(365.10 KB) Additional Information: full citation, abstract, references, index terms

Mobile Ad hoc Networks (MANETs) create additional challenges for implementing the group key establishment due to resource constraints on nodes and dynamic changes on the topology. To facilitate the deployment of group key agreements in MANETs, a range of distributed algorithms have been proposed. However, for a given level of security, these algorithms incur linearly increasing communication and computational costs. In this paper, we present two scalable maximum matching algorithms (M2) to deplo ...

Keywords: group key management, key tree, maximum matching

53 Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks

Haidong Xia, José Carlos Brustoloni
May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**
Publisher: ACM Press
Full text available: pdf(770.11 KB) Additional Information: full citation, abstract, references, index terms

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

Keywords: HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time

instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

54 Security analysis: Privacy enhanced cellular access security

Geir M. Køien
September 2005 **Proceedings of the 4th ACM workshop on Wireless security WiSe '05**
Publisher: ACM Press
Full text available: pdf(230.28 KB) Additional Information: full citation, abstract, references, index terms

The 3G cellular access security architectures do not provide satisfactorily user privacy and fail to fully include all three principal entities involved in the security context. In this paper we propose a beyond-3G Privacy Enhanced 3-Way Authentication and Key Agreement (PE3WAKA) protocol that provides substantially improved user privacy and a 3-way security context. By integrating selected Mobility Management procedures and the PE3WAKA protocol this is achieved with fewer round-trips than the 3 ...

Keywords: access security, entity authentication, wireless privacy

55 Authentication and signature schemes: Efficiency improvements for signature schemes with tight security reductions

Jonathan Katz, Nan Wang
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(306.91 KB) Additional Information: full citation, abstract, references, index terms

Much recent work has focused on constructing *efficient* digital signature schemes whose security is *tightly* related to the hardness of some underlying cryptographic assumption. With this motivation in mind, we show here two approaches which improve both the computational efficiency and signature length of some recently-proposed schemes: **Diffie-Hellman signatures.** Goh and Jarecki [18] recently analyzed a signature scheme which has a tight security reduction to the computational ...

Keywords: digital signatures

56 Extended abstract: New multi-signature and proxy multi-signature schemes from the Weil pairings

Yang Xiaoyuan, Wang Xu-an, Zhang Wei
November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**
Publisher: ACM Press
Full text available: pdf(145.54 KB) Additional Information: full citation, abstract, references, index terms

There exist two classes of proxy multi-signature. In the first class, different proxy signers delegate different original signers, while in the second class a same proxy signer delegates all of the original signers. Based on the bilinear property of the Weil/Tate pairings, consulting Harn's idea of multi-signature and Zhang's method of constructing proxy signature, we constructed new multi-signature and proxy multi-signature schemes covering the first class and the second class. The schemes' sec ...

Keywords: bilinear map, multi-signature, proxy multi-signature, weil/tate pairings

57 Cryptology II: Transformation-free proxy cryptosystems and their applications to electronic commerce

Lihua Wang, Zhenfu Cao, Eiji Okamoto, Ying Miao, Takeshi Okamoto
November 2004 **Proceedings of the 3rd international conference on Information**

security InfoSecu '04

Publisher: ACM Press

Full text available: pdf(648.76 KB) Additional Information: full citation, abstract, references, index terms

In this paper transformation-free proxy cryptosystems (TFP systems) are studied. The TFP system is a modification of the proxy cryptosystem introduced by Mambo and Okamoto [6] in which a ciphertext transformation by the original decryptor is necessary. The TFP system allows proxy decryptor to do decryption without any ciphertext transformation, so that it can release the original decryptor more efficiently from a large amount of decrypting operations. An active identity-based and a directory-bas ...

Keywords: pairing, partial decryption-verification, partial delegation, proxy cryptosystem, transformation-free

Results 41 - 57 of 57 Result page: previous 1 2 **3**

Terms used **identifier based encryption** Found **1** of **193,448**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 1 of 1

Relevance scale

1 Data integrity: The HP time vault service: exploiting IBE for timed release of confidential information

Marco Casassa Mont, Keith Harrison, Martin Sadler
May 2003 **Proceedings of the 12th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(860.87 KB) Additional Information: full citation, abstract, references, index terms

Digital information is increasingly more and more important to enable interactions and transactions on the Internet. On the other hand, leakages of sensitive information can have harmful effects for people, enterprises and governments.This paper focuses on the problems of dealing with timed release of confidential information and simplifying its access once public: it is a common issue in the industry, government and day-to-day life.We introduce the "HP Time Vault Service", based on the emerging ...

Keywords: disclosure policies, identifier-based encryption, privacy, security, timed-release, web service

Results 1 - 1 of 1

Day : Tuesday
Date: 12/26/2006

PALM INTRANET

Time: 10:00:52

Inventor Name Search Result

Your Search was:

Last Name = HARRISON
First Name = KEITH

Application#	Patent#	Status	Date Filed	Title	Inventor Name
06550204	Not Issued	161	11/09/1983	GOLF SWING PRACTICE DEVICE	HARRISON, KEITH
06802173	4743028	150	01/17/1986	GOLF SWING PRACTICE DEVICE	HARRISON, KEITH
07761960	Not Issued	161	03/30/1992	METHOD AND APPARATUS FOR INFORMATION MANAGEMENT IN A COMPUTER DATABASE	HARRISON, KEITH
07761961	Not Issued	166	03/30/1992	METHOD AND APPARATUS FOR GRAPHICAL INTERROGATION OF A DATABASE	HARRISON, KEITH
08428397	5752016	150	04/25/1995	METHOD AND APPARATUS FOR DATABASE INTERROGATION USING A USER-DEFINED TABLE	HARRISON, KEITH
11315633	Not Issued	20	12/22/2005	Authentication method	HARRISON, KEITH
11548251	Not Issued	19	01/01/0001	METHOD OF PROCESSING INFORMATION TO BE CONFIDENTIALLY TRANSMITTED	HARRISON, KEITH
11590493	Not Issued	19	10/30/2006	Methods and systems for executing bit-commitment protocols that are based on entangled quantum states and a third party	HARRISON, KEITH
11343434	Not Issued	25	01/31/2006	Methods and systems for avoiding transmission-channel disruptions	HARRISON, KEITH A.
08435490	5691917	150	05/05/1995	EVENT-PROCESSING SYSTEM AND METHOD OF CONSTRUCTING SUCH A SYSTEM	HARRISON, KEITH A.
09852262	6941476	150	05/10/2001	INFORMATION STORAGE	HARRISON, KEITH ALEXANDER

09897416	7065656	150	07/03/2001	TAMPER-EVIDENT/TAMPER-RESISTANT ELECTRONIC COMPONENTS	HARRISON, KEITH ALEXANDER
09897424	Not Issued	71	07/03/2001	Tamper-evident and/or tamper-resistant electronic components	HARRISON, KEITH ALEXANDER
09918062	Not Issued	41	07/30/2001	AUTHENTICATING FACSIMILE DOCUMENTS USING DIGITAL SIGNATURES	HARRISON, KEITH ALEXANDER
09918188	Not Issued	83	07/30/2001	Document transmission Techniques I	HARRISON, KEITH ALEXANDER
09918326	Not Issued	123	07/30/2001	Document Transmission techniques II	HARRISON, KEITH ALEXANDER
09955222	Not Issued	120	09/19/2001	Credential transfer methods	HARRISON, KEITH ALEXANDER
10023846	Not Issued	83	12/21/2001	Methods of communication	HARRISON, KEITH ALEXANDER
10023887	Not Issued	61	12/21/2001	Communication methods, communication systems and to personal communication devices	HARRISON, KEITH ALEXANDER
10053522	Not Issued	161	01/23/2002	Base station/data storage	HARRISON, KEITH ALEXANDER
10079598	7107250	150	02/19/2002	APPARATUS FOR CREDENTIAL AUTHORISATION	HARRISON, KEITH ALEXANDER
10096290	Not Issued	161	03/12/2002	Method and apparatus for configuring a portable computing device	HARRISON, KEITH ALEXANDER
10120140	Not Issued	93	04/11/2002	DATA AUTHENTICATION	HARRISON, KEITH ALEXANDER
10245732	Not Issued	83	09/17/2002	Long-term storage and renewal of encrypted data	HARRISON, KEITH ALEXANDER
10270037	Not Issued	41	10/11/2002	Method and apparatus for encrypting data	HARRISON, KEITH ALEXANDER
10270039	Not Issued	61	10/11/2002	Method and apparatus for encrypting data	HARRISON, KEITH ALEXANDER
10270040	Not Issued	61	10/11/2002	Method and apparatus for encrypting data	HARRISON, KEITH ALEXANDER
10298735	Not Issued	41	11/18/2002	Digital certificate verification	HARRISON, KEITH ALEXANDER
10313868	Not Issued	41	12/06/2002	Apparatus for setting access requirements	HARRISON, KEITH ALEXANDER
10317536	7146495	150	12/12/2002	DIGITAL DOCUMENT STORAGE	HARRISON, KEITH ALEXANDER
10336590	7086052	150	01/03/2003	SOFTWARE INSTALLATION AND OPERATION WITH RANDOM SELECTION	HARRISON, KEITH ALEXANDER

10379455	Not Issued	71	03/03/2003	Method and apparatus for encrypting/decrypting data	HARRISON, KEITH ALEXANDER
10414993	Not Issued	121	04/16/2003	Long-term digital storage	HARRISON, KEITH ALEXANDER
10437976	Not Issued	30	05/15/2003	Distributed processing	HARRISON, KEITH ALEXANDER
10613522	Not Issued	71	07/02/2003	Method and apparatus for use in relation to verifying an association between two parties	HARRISON, KEITH ALEXANDER
10613750	Not Issued	30	07/03/2003	Method and apparatus for generating a cryptographic key	HARRISON, KEITH ALEXANDER
10623008	Not Issued	30	07/17/2003	Method and apparatus for securely transferring data	HARRISON, KEITH ALEXANDER
10664069	Not Issued	30	09/16/2003	Data output method, system and apparatus	HARRISON, KEITH ALEXANDER
10697272	Not Issued	41	10/31/2003	Secure physical documents, and methods and apparatus for publishing and reading them	HARRISON, KEITH ALEXANDER
10767868	Not Issued	30	01/28/2004	Privacy management of personal data	HARRISON, KEITH ALEXANDER
10829930	Not Issued	30	04/21/2004	Security method and apparatus using biometric data	HARRISON, KEITH ALEXANDER
10829931	Not Issued	30	04/21/2004	Security method and apparatus using biometric data	HARRISON, KEITH ALEXANDER
10831350	Not Issued	30	04/22/2004	Cryptographic method and apparatus	HARRISON, KEITH ALEXANDER
10831548	Not Issued	30	04/22/2004	Cryptographic method and system	HARRISON, KEITH ALEXANDER
10831549	Not Issued	30	04/22/2004	Cryptographic method and apparatus	HARRISON, KEITH ALEXANDER
10831776	Not Issued	30	04/22/2004	Cryptographic method and apparatus	HARRISON, KEITH ALEXANDER
10848570	Not Issued	71	05/19/2004	Method and product for sharing logged data objects within a distributed storage system	HARRISON, KEITH ALEXANDER
10866053	Not Issued	30	06/10/2004	RSA cryptographic method and system	HARRISON, KEITH ALEXANDER
10868743	Not Issued	30	06/14/2004	Mediated RSA cryptographic method and system	HARRISON, KEITH ALEXANDER
10893571	Not Issued	30	07/15/2004	Trusted authority for identifier-based cryptography	HARRISON, KEITH ALEXANDER

Search and Display More Records.

Search Another: Inventor Last Name HARRISON First Name KEITH Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

Day : Tuesday
Date: 12/26/2006

PALM INTRANET

Time: 10:01:03

Inventor Name Search Result

Your Search was:

Last Name = HARRISON
First Name = KEITH

Application#	Patent#	Status	Date Filed	Title	Inventor Name
10941262	Not Issued	25	09/14/2004	Secure provision of image data	HARRISON, KEITH ALEXANDER
10982500	Not Issued	30	11/05/2004	Smartcard with cryptographic functionality and method and system for using such cards	HARRISON, KEITH ALEXANDER
11150623	Not Issued	30	06/10/2005	Cryptographic method and apparatus	HARRISON, KEITH ALEXANDER
11166921	Not Issued	30	06/23/2005	Cryptographic method and apparatus	HARRISON, KEITH ALEXANDER
11182527	Not Issued	30	07/14/2005	Identifier-based signcryption with two trusted authorities	HARRISON, KEITH ALEXANDER
11305869	Not Issued	30	12/16/2005	Method and apparatus for generating an identifier-based public/private key pair	HARRISON, KEITH ALEXANDER
11316412	Not Issued	25	12/21/2005	Use of Bilinear mappings in cryptographic applications	HARRISON, KEITH ALEXANDER
11454624	Not Issued	25	06/16/2006	Quantum key distribution apparatus & method	HARRISON, KEITH ALEXANDER
11454632	Not Issued	25	06/16/2006	Quantum key distribution method and apparatus	HARRISON, KEITH ALEXANDER
11455231	Not Issued	25	06/16/2006	Method and device using one-time pad data	HARRISON, KEITH ALEXANDER
11455317	Not Issued	30	06/19/2006	Secure transaction method and transaction terminal for use in implementing such method	HARRISON, KEITH ALEXANDER
11481797	Not Issued	25	07/07/2006	Pharmaceutical product packaging	HARRISON, KEITH ALEXANDER
11489750	Not Issued	19	07/17/2006	Method of managing one-time pad data and device implementing this method	HARRISON, KEITH ALEXANDER
11490478	Not Issued	20	07/19/2006	Method of operating a one-time pad system and a system for implementing this method	HARRISON, KEITH ALEXANDER
11490852	Not Issued	25	07/21/2006	Method of provisioning devices with one-time pad data, device	HARRISON, KEITH ALEXANDER

				for use in such method, and service usage tracking based on one-time pad data	
11490853	Not Issued	25	07/21/2006	Device with multiple one-time pads and method of managing such a device	HARRISON, KEITH ALEXANDER
11493031	Not Issued	19	07/26/2006	Physical items for holding data securely, and methods and apparatus for publishing and reading them	HARRISON, KEITH ALEXANDER
11523868	Not Issued	25	09/19/2006	Method and system using one-time pad data to evidence the possession of a particular attribute	HARRISON, KEITH ALEXANDER
09483800	Not Issued	71	01/15/2000	PROVISION OF TRUSTED SERVICES	HARRISON, KEITH ALEXANDER
60167892	Not Issued	159	11/30/1999	INTERNET CUSTOMER DIRECTED CHARITABLE COMMERCE SYSTEM	HARRISON, KEITH J.
08669156	Not Issued	160	06/24/1996	VENDING MACHINE CASH	HARRISON, KEITH L
07424704	Not Issued	166	10/20/1989	SHELL MOULDS	HARRISON, KEITH L.
07630775	Not Issued	164	12/21/1990	SHELL MOULDS	HARRISON, KEITH L.
06156584	4322485	150	06/05/1980	THE PREPARATION OF MATERIALS	HARRISON, KEITH T.

Inventor Search Completed: No Records to Display.

Search Another: Inventor

Last Name: HARRISON

First Name: KEITH

Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

Day : Tuesday
Date: 12/26/2006

PALM INTRANET

Time: 10:02:58

Inventor Name Search Result

Your Search was:

Last Name = CHEN
First Name = LIQUN

Application#	Patent#	Status	Date Filed	Title	Inventor Name
09306112	Not Issued	161	05/06/1999	FAIR EXCHANGE OF DIGITAL SIGNATURES IN COMMUNICATIONS NETWORK	CHEN, LIQUN
09913452	6988250	150	12/05/2001	TRUSTED COMPUTING PLATFORM USING A TRUSTED DEVICE ASSEMBLY	CHEN, LIQUN
09913454	Not Issued	120	08/14/2001	Protection of the configuration of modules in computing apparatus	CHEN, LIQUN
09931526	Not Issued	120	08/16/2001	Apparatus and method for establishing trust	CHEN, LIQUN
09932476	Not Issued	61	08/17/2001	Trusted system	CHEN, LIQUN
09936132	7069439	150	09/04/2001	COMPUTING APPARATUS AND METHODS USING SECURE AUTHENTICATION ARRANGEMENTS	CHEN, LIQUN
09946323	Not Issued	120	09/04/2001	Method and apparatus for using a secret in a distributed computing system	CHEN, LIQUN
09979904	Not Issued	41	11/27/2001	System for digitally signing a document	CHEN, LIQUN
09979905	Not Issued	120	11/27/2001	System for providing a trustworthy user interface	CHEN, LIQUN
10088258	Not Issued	61	03/13/2002	Trusted computing platform for restricting use of data	CHEN, LIQUN
10110279	Not Issued	61	07/12/2002	Trusted computing platform with biometric authentication	CHEN, LIQUN
10110280	7096204	150	08/23/2002	ELECTRONIC COMMERCE SYSTEM	CHEN, LIQUN
10175183	7076655	150	06/18/2002	MULTIPLE TRUSTED COMPUTING ENVIRONMENTS WITH VERIFIABLE ENVIRONMENT IDENTITIES	CHEN, LIQUN

10175542	Not Issued	71	06/18/2002	Multiple trusted computing environments	CHEN, LIQUN
10194831	Not Issued	61	07/11/2002	Trusted platform evaluation	CHEN, LIQUN
10208718	Not Issued	71	07/29/2002	Method and apparatus for locking an application within a trusted environment	CHEN, LIQUN
10270040	Not Issued	61	10/11/2002	Method and apparatus for encrypting data	CHEN, LIQUN
10344062	Not Issued	71	01/07/2004	Trusted device	CHEN, LIQUN
10371125	Not Issued	61	02/20/2003	Systems and methods for enhanced image adaptation	CHEN, LIQUN
10415449	Not Issued	30	10/24/2003	Metering in a data processing system	CHEN, LIQUN
10557953	Not Issued	19	01/01/0001	Use of certified sectrets in communication	CHEN, LIQUN
10613522	Not Issued	71	07/02/2003	Method and apparatus for use in relation to verifying an association between two parties	CHEN, LIQUN
10613750	Not Issued	30	07/03/2003	Method and apparatus for generating a cryptographic key	CHEN, LIQUN
10623008	Not Issued	30	07/17/2003	Method and apparatus for securely transferring data	CHEN, LIQUN
10664069	Not Issued	30	09/16/2003	Data output method, system and apparatus	CHEN, LIQUN
10676518	Not Issued	41	09/30/2003	Document representation for scalable structure	CHEN, LIQUN
10782079	Not Issued	25	02/19/2004	Limiting service provision to group members	CHEN, LIQUN
10797715	Not Issued	30	03/08/2004	Method, system and device for enabling delegation of authority and access control methods based on delegated authority	CHEN, LIQUN
10825596	Not Issued	30	04/14/2004	Secure data provision method and apparatus and data recovery method and system	CHEN, LIQUN
10829930	Not Issued	30	04/21/2004	Security method and apparatus using biometric data	CHEN, LIQUN
10829931	Not Issued	30	04/21/2004	Security method and apparatus using biometric data	CHEN, LIQUN
10831350	Not Issued	30	04/22/2004	Cryptographic method and apparatus	CHEN, LIQUN
10831548	Not Issued	30	04/22/2004	Cryptographic method and system	CHEN, LIQUN
10831549	Not Issued	30	04/22/2004	Cryptographic method and apparatus	CHEN, LIQUN

10831776	Not Issued	30	04/22/2004	Cryptographic method and apparatus	CHEN, LIQUN
10866053	Not Issued	30	06/10/2004	RSA cryptographic method and system	CHEN, LIQUN
10868743	Not Issued	30	06/14/2004	Mediated RSA cryptographic method and system	CHEN, LIQUN
10893571	Not Issued	30	07/15/2004	Trusted authority for identifier-based cryptography	CHEN, LIQUN
10957014	Not Issued	30	09/30/2004	Digital signature method and apparatus	CHEN, LIQUN
10977342	Not Issued	30	10/29/2004	Identifier-based signcryption	CHEN, LIQUN
10982500	Not Issued	30	11/05/2004	Smartcard with cryptographic functionality and method and system for using such cards	CHEN, LIQUN
11150623	Not Issued	30	06/10/2005	Cryptographic method and apparatus	CHEN, LIQUN
11166921	Not Issued	30	06/23/2005	Cryptographic method and apparatus	CHEN, LIQUN
11182527	Not Issued	30	07/14/2005	Identifier-based signcryption with two trusted authorities	CHEN, LIQUN
11249820	Not Issued	30	10/12/2005	Trusted computing platform	CHEN, LIQUN
11305869	Not Issued	30	12/16/2005	Method and apparatus for generating an identifier-based public/private key pair	CHEN, LIQUN
11315633	Not Issued	20	12/22/2005	Authentication method	CHEN, LIQUN
11316412	Not Issued	25	12/21/2005	Use of Bilinear mappings in cryptographic applications	CHEN, LIQUN
11454632	Not Issued	25	06/16/2006	Quantum key distribution method and apparatus	CHEN, LIQUN
11481797	Not Issued	25	07/07/2006	Pharmaceutical product packaging	CHEN, LIQUN

Search and Display More Records.

Search Another: Inventor Last Name CHEN First Name LIQUN Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

Day : Tuesday
Date: 12/26/2006

PALM INTRANET

Time: 10:03:04

Inventor Name Search Result

Your Search was:

Last Name = CHEN
First Name = LIQUN

Application#	Patent#	Status	Date Filed	Title	Inventor Name
11493910	Not Issued	25	07/25/2006	Data transfer system	CHEN, LIQUN
11493972	Not Issued	19	07/27/2006	Methods and systems for utilizing cryptographic functions of a cryptographic co-processor	CHEN, LIQUN
11548251	Not Issued	19	01/01/0001	METHOD OF PROCESSING INFORMATION TO BE CONFIDENTIALLY TRANSMITTED	CHEN, LIQUN
11351528	Not Issued	30	02/10/2006	Microarchitectural wire management for performance and power in partitioned architectures	CHENG, LIQUN
11394503	Not Issued	30	03/31/2006	Preselecting E/M line replacement technique for a snoop filter	CHENG, LIQUN
11395123	Not Issued	30	03/31/2006	Way hint line replacement algorithm for a snoop filter	CHENG, LIQUN
11413620	Not Issued	20	04/28/2006	Apparatus and method of controlling data sharing on a shared memory computer system	CHENG, LIQUN
11479327	Not Issued	30	06/29/2006	Exclusive ownership snoop filter	CHENG, LIQUN

Inventor Search Completed: No Records to Display.

Search Another: Inventor Last Name: CHEN First Name: LIQUN Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page